經濟部 110 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》
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　110 年 3 月 22 日

110年度合作研究計畫建議書徵求文件

一、 簡介

在萬物聯網的時代，各類資訊系統與物聯網裝置深入每個人的生活，而為了資訊安全及個人隱私的防護，密碼演算法的實作是資訊系統或裝置設計中不可或缺的一環。依據實作方式，密碼模組可分為在微處理器上的軟體實作與特製的密碼硬體電路兩大類，而不論何種實作方式，最終密碼演算法都必須在硬體晶片上執行運算，因此，這類設計除了兼顧速度與節能的考量之外，最重要的是必須考慮各種針對密碼硬體的資安攻擊。

旁通道攻擊(Side Channel Attack, SCA)是藉由蒐集硬體裝置進行密碼運算時不經意洩漏之物理訊號，以統計與信號處理等技術分析而得到祕密資訊，這種方法繞過密碼理論的防護，即使是數學理論上被證明為安全的加密演算法亦可能被攻擊，其攻擊力強且不限定攻擊特定密碼系統，且可能被利用之旁通道洩溢包括能量消耗、電磁輻射、運算時間、聲音等物理訊號，只要實作上稍不注意，任何密碼硬體裝置都可能在不同的旁通道上提供破密者有用的資訊，使得這類裝置的安全性受到相當大的威脅。

有鑑於破密能力越來越強的SCA技術不斷被提出，SCA防護能力檢測必然成為密碼硬體安全鑑測的重點項目，在美國國家標準局(NIST)針對密碼模組的認證標準中已明列對於SCA的防護為其中要項。目前針對SCA防護能力檢測主要分為兩類方法，第一類是實測評估法(evaluation-style testing)，亦即以已知所有最先進的SCA方法進行實際攻擊，採用這類方法是Common Criteria (CC)認證，它的好處是能夠直接得知待測裝置對不同攻專的抵禦能力，但這種方法對於檢測人員的技術要求較高；第二類是符合性測試(conformance-style testing)，這是以標準化的統計方法評定待測裝置的旁通道洩溢是否低於容許值，採用這類方法的是FIPS認證，它能以標準化的流程施測，對於檢測實驗室之建立與施測人員技術要求較低，可以較低成本達成高效檢測之目標，易於大量檢測，不過目前為止，這類檢測的最大問題就是尚未找到能直接將檢測結果對應至裝置之SCA抵禦能力的方法，符合性測試不通過並不代表有SCA方法能成功破密，反之亦然。

因此，如何進一步找到兩類檢測方法的轉換方式，或者找出能直接轉換的符合性測試指標，將會是一項重大突破。目前為止，不論是FIPS 140-2或FIPS 140-3中均仍未明確訂定旁通道抵禦能力檢測之標準方法與指標，在學界與業界較常被使用及討論的數種以統計方法所計算之指標，如Test Vector Leakage Assessment (TVLA)、Normalized Inter-Class Variance (NICV)、Signal-to-Noise Ratio (SNR)都各有其優缺點，亟需更多的實測與理論研究來完善這類檢測方法。再者，目前國內針對密碼硬體之SCA防護能力檢測需求多要仰賴國外大廠之設備與技術，如何建立完整檢測環境並培養相關人才也是提昇整體檢測技術當務之急。

二、 計畫目標

本計畫將實作並評估硬體晶片之旁通道洩溢檢測技術，目標以研究目前文獻中所提出之統計檢測指標與實測SCA抵禦能力之關聯性為主，預計以業界普遍使用之嵌入式系統處理器上之常用加解密演算法實作為實測標的，實測之SCA方法為常用之profiling attacks或non-profiling attacks，以期能獲得具廣泛應用價值之結果，提供旁通道洩溢檢測標準建立之參考。

三、 計畫範圍

本計畫預計研究以下主要項目：

- 針對硬體晶片之能量消耗與電磁輻射等旁通道訊號軌跡處理與洩溢檢測之軟體實作
- 研析洩溢檢測指標與SCA抵禦能力之關聯性，包含profiling與non-profiling attacks，並以ARM核心處理器上之加解密演算法實作為優先研析對象

四、 預期成果

本計畫須配合母計畫需要進行研發，並產出以下成果：

- 於110年7月底交付針對硬體晶片之能量消耗與電磁輻射等旁通道訊號軌跡處理與洩溢檢測之軟體模組原始碼，功能至少包含TVLA、NICV、SNR之計算。
- 於110年11月底交付一篇洩溢檢測指標與SCA抵禦能力之關聯性實測研析報告書。

※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。

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，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為主。

六、 計畫期程及預估計畫總經費

計畫執行區間： 110 年 4 月 1 日 至 110 年 12 月 15 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章「預期成果」規定，如期繳交相關成果。

八、 技術能力需求(請詳述所需要之技術能力或專長)

- 具硬體晶片旁通道攻擊實測研究經驗之學界研究人員。
- 熟悉硬體晶片之CC與FIPS140-2/140-3相關資安認證之學界研究人員
- 熟悉硬體資安相關背景知識，並具備相關軟硬體實作經驗之技術人員