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

《晶片電路量化資料流弱點檢測研究計畫》

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 18 日

111 年度合作研究計畫建議書徵求文件

一、 簡介

近年來，隨著物聯網（Internet of Things, IoT）技術的發展並與人工智慧、擴增實境、5G 通訊技術等科技的結合，許多創新的物聯網裝置也隨之被提出並深入在每個人的生活中。而在物聯網技術普及的過程中，資訊安全的風險逐漸提高，其中，在資訊安全防護以及個人隱私保護這些重要的議題中，密碼學演算法扮演不可或缺的角色。目前的加密方式主要可以分成硬體加密以及軟體加密，而這兩種方式都是需要在硬體晶片上進行執行計算才能實現密碼學演算法。在密碼學演算法的設計中，除了要考量到效率、效能與靈活性以外，最重要的是要能夠在滿足資訊安全三要素 CIA (Confidentiality, Integrity, and Availability)的狀況下還能夠去抵禦密碼硬體攻擊。

現今針對密碼硬體的旁通道攻擊(Side-Channel Attack, SCA)已成為密碼硬體裝置的一大威脅。旁通道攻擊不需要破壞硬體裝置，透過量測和分析硬體裝置在進行密碼學演算法的過程中物理訊號所洩漏的資訊，進而取得硬體裝置的秘密訊息。不同於以往其他針對密碼學演算法漏洞的攻擊方式，這種攻擊方式可以繞過理論分析上安全的密碼學演算法，極難防範且其攻擊目標不僅限於密碼硬體。在硬體架構設計漏洞或是實作上稍有缺失的狀況下，只要藉由分析旁通道訊號的洩溢，像是功率消耗、電磁輻射、時間資訊和聲音等的物理資訊的洩漏，破密者就有機會在密碼硬體裝置的旁通道上取得秘密資訊，造成這些裝置的安全性受到極大的威脅。

因此，對於密碼硬體受到旁通道攻擊的防護能力檢測已然成為重要項目之一。目前針對密碼硬體對旁通道攻擊的防護能力驗證及評估的方法主要可以分成兩種，第一種是實測評估法(evaluation-style testing)，而在實測評估法中，共同準則(Common Criteria, CC)是一個典型的例子，針對目前所有最先進的旁通道攻擊進行評估，然而這種方式的測試方法繁瑣、成本高昂且對於專業知識的要求較高。第二種是符合性測試法(conformance-style testing)，其中一個例子是 FIPS 認證，它是使用加密模組驗證程式來驗證目標是否符合安全需求，對於旁通道攻擊方面，它僅檢測有哪些洩漏的存在，因此成本較低且對於專業知識的需求較低，可應用於大量檢測。

然而，上述評估能量消耗旁通道（power side-channel attack）訊號洩溢的工具被限制於須利用實際的硬體去做檢測，雖然於矽後階段做評估之時間花費遠遠少於矽前階段，且兩者之準確率差異往往十分巨大，但在矽後階段才進行旁通道訊號洩溢之檢測，對電路設計來說是非常不具靈活性的。

二、 計畫目標

因此在此計畫中，我們希望達到有效率、準確率高，同時能在矽前設計階段,就完成能量消耗旁通道訊號洩溢之評估,以期在電子設計自動化(EDA)廣泛被應用之現況，能達到可以靈活且即時去修正電路之成果，同時能降低對於能量消耗旁通道訊號洩溢之成本。

本計畫目標為於矽前(Pre-silicon)設計階段實作其電路之能量消耗旁通道訊號洩溢評估，需使用矽前模擬工具作為輔助，生成電路資訊作為資料輸入，目前文獻中有使用資訊流（IFT）[1]、統計指標[2]來實作評估計算，但並無將兩者做整合之實作方法，因此在本計畫中，希望能將兩者整合，並預計使用常見加密技術之電路及其改良電路作為實測標的，以期能獲得具廣泛應用價值之結果，於矽前設計階段提供旁通道洩溢之評估工具。

三、 計畫範圍

本計畫預計研究以下主要項目：

- 針對硬體電路之能量消耗旁通道訊號洩溢於矽前設計階段檢測之架構及軟體實作
- 研析洩溢檢測指標與抵禦能力之關聯性，並以加解密電路之暫存器傳輸級(RTL)為優先研析對象

四、 預期成果

本計畫須配合主計畫需要進行研發，並產出以下成果：

1. 此計畫需配合產出至少一篇論文
2. 於 111 年 9 月 30 日交付期中報告一篇，包含以下項目：
   A. 電路模擬及生成所需資訊之系統架構圖及使用說明
   B. 生成 Testbench 之程式原始碼
   C. 測試電路之 RTL 檔、Testbench、.saif 檔及相關資料
   D. 矽前階段功耗旁通道攻擊脆弱性評估之程式原始碼及架構圖
   E. 20 組(含)以上的測試電路評估結果及其分析報告

3. 於 111 年 11 月 30 日交付期末報告一篇，包含以下項目：

A. 經改進之功耗旁通道攻擊脆弱性評估程式原始碼

B. 系統、軟體及程式之使用說明文件

C. 改進方法及其分析報告

※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為主。

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(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。
- 熟悉電路模擬工具並具備實際操作或研究經驗的研究人員。
- 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。