經濟部109年度
提升IC晶片軟體安全品質(BSIMM)與合規技術研發計畫
合作研究計畫

資安防護晶片場域建置計畫

建議書徵求文件

財團法人資訊工業策進會

中華民國 109 年 00月 00 日

109年度合作研究計畫建議書徵求文件

一、 簡介

NoC、Chiplet異質封裝等技術被視為是未來AI, 5G時代之重要技術，然而新的技術架構亦帶來新的資安議題。例如NoC電路IP間是否隱藏著未知的威脅，不同的電路IP通常由不相同的部門甚至於公司所提供，其利用晶片上網路進行相互間的資料傳輸，若某個電路IP例如MCU被置入惡意程式，或是傳輸IP被置入硬體木馬，則晶片雖仍正常操作，但實則已是僵屍晶片。而Chiplet亦面臨同樣嚴重的問題，若採用的小晶片遭受上述惡意攻擊亦無法幸免，更不用說市面上已出現許多假晶片，若封裝中採用了假晶片，可以想見其將出現更為嚴重的資安攻擊。這些資安威脅的可能性也已被許多單位在會議及期刊中批露並重視。解決上述問題的可能方法需要完善的資安防護手段，必需考量在完整設計生命週期各階段注入相對應的資安防護技術，以晶片設計為例，由晶片規畫至設計、佈局、製作到封裝販售，甚至於系統應用，均需有相對應的資安防護考量。而採用硬體防護技術如物理不可複製晶片(PUF; Physical Unclonable Function)進行防護被視為未來台灣最有可能發展的晶片防護技術之一而備受重視。

PUF是利用元件在製造期間無可避免的微小製程變異，例如元件在臨界切換時無法預測的的隨機切換特性，元件先天呈現隨機分布的特性等機制，來使硬體產生如人類指紋般獨一無二的晶片特徵，其所產生的晶片特徵碼具備不可預測性、真隨機亂數等特性，進而可作為無法被仿製的金鑰，來提升晶片端的資安層次。目前PUF技術相當多元，常見有基於CMOS邏輯與基於非揮發性記憶體(NVM)等兩類，其中CMOS邏輯的PUF技術主要是依靠製程變異，並藉由後續的放大設計來達成PUF功能，而NVM的PUF技術則亦採前述方法來達成。目前CMOS邏輯的PUF技術因具有與CMOS完全相容的特點，所以發展較為快速，已有相關商品，而NVM的PUF技術也已有基於現有記憶體架構而被提出的，如：OTP、Flash等技術的PUF產品，例如國內廠商力旺所開發的NeoPUF即為其中之一。

然而，如PUF之類硬體防護技術目前處於開始應用階段，仍有著許多問題等待解決，例如目前PUF通常被視為一晶片身份證使用，但其傳輸認證方式並未統一。且PUF天生亂數的特性，亦可作為傳輸時之加解密使用，但相對應之傳輸電路以及加解密演算法亦仍處於開發階段，亦是現在熱門的研究主題。除了技術面的問題外，沒有通過資安認證(例如FIPS140-2)的產品，其防護能力是受到質疑的，以美國為例，公務機關所採購之資安物品必需通過FIPS 140-2認證才可，顯見資安認證之必要性，因此應用硬體防護技術之產品如何進行資安認證，亦是極需重視的問題。

二、 計畫目標

本計畫將對於硬體防護技術如PUF之防護手段及其國際認證標準進行評估和研析，目標為研析如何以硬體防護技術加強晶片產品之資安防護能力為主，並以實際處理器所可能面臨之惡意威脅作為參考，評估硬體防護技術之可能解法；另外亦將針對硬體防護技術之國際認證如 FIPS140-2 作一研析，以使未來使用此解法之產品能藉由認證進行產品加值及區隔。

三、 計畫範圍

本計畫預計研究以下主要項目：

- FIPS140-2 認證與硬體資安防護晶片(PUF)新型防護技術研析

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109年11月底交付晶片韌體標準開發階段性產出5隻以上檔案(firmware design files)一案。
- 於109年11月底交付晶片標準開發階段性產出驗證檔案(IC design files)一案。
- 於109年11月底交付硬體防護技術及其認證標準研析報告書一份。

※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： 109 年 7 月 1 日 至 109 年 12 月 15 日

總經費：1,500,000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。

1.晶片韌體標準開發階段性產出檔案包括：標準IoT系統韌體設計平台(arduino, TI…)等具無線連結操作之韌體設計相關檔案。

2.晶片標準開發階段性產出驗證檔案包括：標準FPGA 設計、Cell based IC 設計以及ASIC設計等通用晶片設計相關檔案。

3.硬體防護技術及其驗證標準研析報告書需包含以下研究內容：(1)簡介；(2)硬體防護技術研析；(3)認證標準研析；(4)硬體防護技術認證研析；(5)結論

八、 技術能力需求

- 具ASIC電路設計、Cell based IC設計整合晶片硬體防護技術(如PUF)之晶片實際下線、製作及量測驗證經驗之技術研發人員。
- 具備且熟悉資安認證標準(如FIPS140-2)及認證流程之技術研發人員。
- 熟悉資安相關背景知識領域，並對系統攻防，弱點防禦，或惡意軟體等有實際操作或研究經驗的技術人員。

附件1：契約書格式
1-1：計畫書格式
1-2：經費動支報表
1-3：成果報告撰寫須知
1-4：報告格式
1-5：論文格式
1-6：保密聲明書
1-7：委託匯款同意書