基於可信任平台模組晶片之軟體智財保護

國立高雄科技大學第一校區
指導教授　：陳朝烈
學生　　：林子豪

壹、摘要：

資訊技術不斷進步，使得軟體程式應用面以及商品愈來愈多，軟體程式的開發需要耗費大量資源，然而，軟體盜版和非法使用卻也愈加嚴重，這些問題會對軟體開發商造成巨大的經濟損失，因此，軟體開發商需要建立保護措施以此面對層出不窮的破解以及適應不同的軟體執行環境以避免漏洞，本專題利用TPM(Trusted Platform Module)晶片模組建立一個軟體商品程式保護方式，TPM是一種硬體式安全晶片，其設計目的是提供一個安全的環境，以保護電腦系統免受攻擊、入侵、串改，每個TPM在生產時都各自綁定一組唯一的非對稱式密鑰，並儲存在TPM晶片的不可讀區域中，並且無法透過任何方式獲取根密鑰，利用TPM除了能達到軟體商品啟動防盜以外，也能對AI模型加密以達到保護其內各種資訊，API的形式搭配TPM的特性使得該專題於各種本地端的加密及驗證都能產生作用。

貳、同類型方法分析：

特性/方法	授權金鑰	USB 授權	雲端授權	HSM	FPGA	本專題
無網路需求(初次)		✓		✓	✓	✓
無網路需求(常態)	✓	✓		✓	✓	✓
無須連接外部硬體	✓		✓			✓
不受斷電影響	✓		✓	✓	✓	✓
不受更換硬體影響		✓	✓	✓		✓

註:HSM(Hardware Security Module)
FPGA(Field Programmable Gate Array)

參、專題優缺分析：

優點:

1.硬體層面保護：和HSM、FPGA比起，並不需要額外物理連結和接線

2.**高彈性**：由於將專題模組化，於不同的程式內直接呼叫API就能達到驗證功能(該設備有TPM)

3.**唯一性**：由於將程式與設備綁定，就算將程式移植到其他設備上使用也無法正常執行，同一程式只有唯一一個使用者(設備)

4.**操作需要密碼**：密碼包括在API內，是為了防止駭客跳過程式自行對tpm進行指令操作，產品程式使用者並不需要額外操作

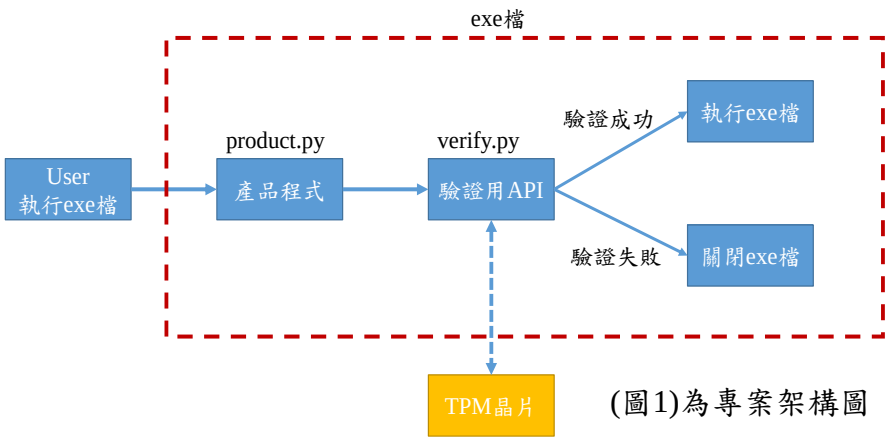
5.**無須網路環境執行**

6.**不受斷電影響**

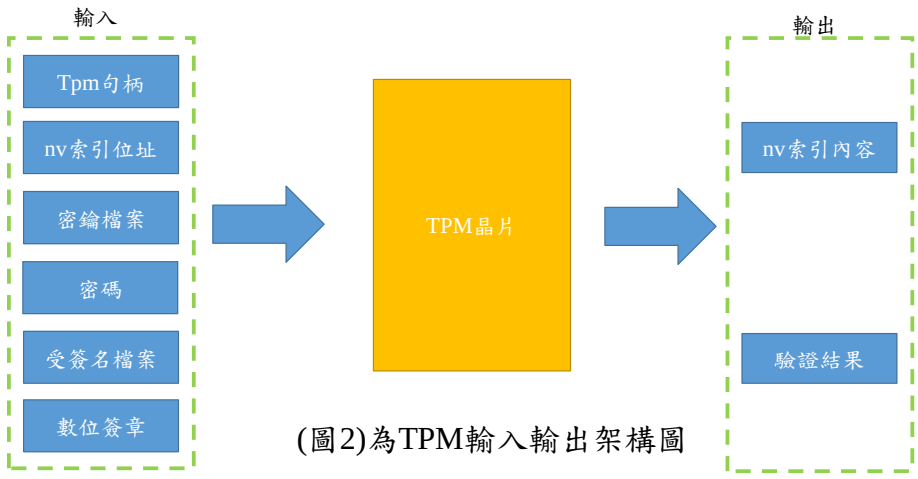
缺點:

1.驗證用檔案遺失就需要重新手動設定

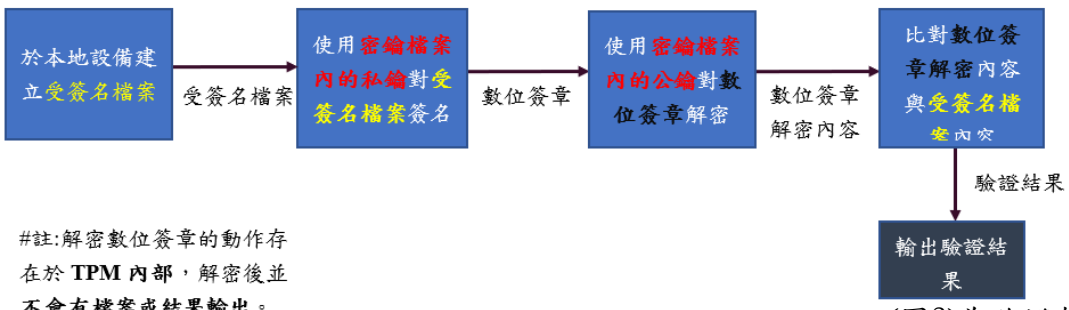
肆、系統架構：



(圖1)為專案架構圖



(圖2)為TPM輸入輸出架構圖



#註:解密數位簽章的動作存在於 **TPM 內部**，解密後並**不會有檔案或結果輸出**。

(圖3)為驗證架構圖

(圖4)為TPM晶片正面圖

(圖5)為TPM晶片反面圖

TPM出廠前放置在設備內，不須使用者額外操作(手動驗證、插USB)

流程內所用到的檔案、金鑰以及執行動作都存在於TPM內部，此外，TPM內部儲存空間部份不受斷電以及電腦重開機的影響。透過程式與TPM進行操作，達到硬體設備的綁定。為了防止駭客可能嘗試跳過程式，自行對TPM進行任何破解或操作的風險，於出貨前對TPM設定綁定一組自行設定的密碼，此密碼並不會在任何情況下於外部被獲取。程式部分寫成API，方便彈性使用於任何需要保護軟體的情境。