國科會臺灣資安科技研究中心專案計畫

計畫名稱：關鍵基礎設施的資訊安全防護機制設計—基於身分認證及可信度驗證之晶片安全設計方法

計畫主持人：王行健(國立中興大學)　　計畫編號：NSTC 112-2634-F-005-001-MBK

[子一]：基於可信度認證與驗證之晶片安全設計

王行健(中興資工)、李淑敏(中山資工)

1. 技術摘要

旁通道分析（SCA）是針對密碼設備執行加密操作所洩漏的實體訊號，透過統計和訊號處理技術分析得到密鑰。

本計畫提出三項輕量級的反制方式以提高AES加密模組的抗SCA能力。

① **管線執行**

② **SubBytes偏移執行次序(Skewed Execution Order)**

③ **均衡化AddRoundKey的漢明權重**

2. 技術亮點/突破點：抗SCA能力評估結果

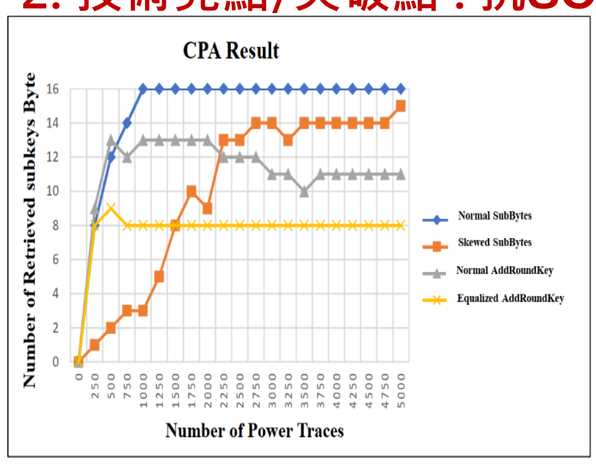


Fig. 1. CPA results against AES designs with 4 LUTs.

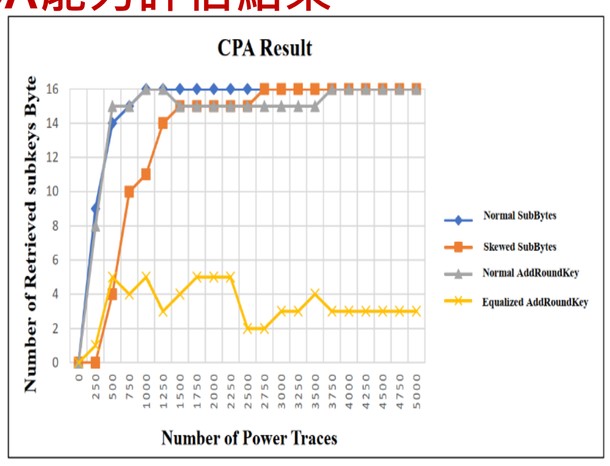


Fig. 2. CPA results against AES designs with 8 LUTs.

[子二]：物聯網裝置加密器晶片

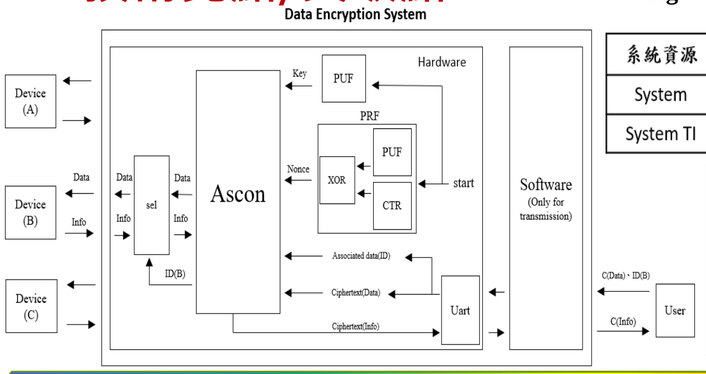
賴永康、林泓均 (中興電機)

1. 技術摘要

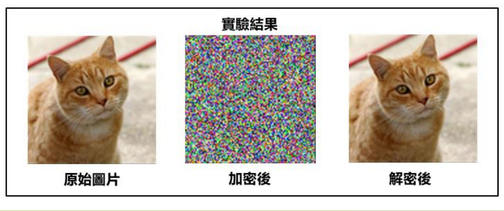
基於PUF和Ascon的資料傳輸加密系統於FPGA上實現，結合兩種技術創建一個更加堅固、可靠的物聯網安全環境。不僅提高資料安全性，更加安全的使用體驗。經過文獻探討與分析，密碼系統選擇輕量級密碼標準Ascon，而PUF選擇使用Weak PUF類型的NAND PUF & XOR PUF，並將其合成實現並燒錄在FPGA(Nexys 4 DDR Artix-7) 。

2. 技術亮點/突破點：

Fig. 3. 系統架構圖與實驗結果圖



系統資源	Utilization(LUT)(%)	Utilization(FF)(%)	Power(W)
System	3649/63400(5.8%)	2373/126800(1.9%)	0.142
System TI	11389/63400(18%)	5455/126800(4.3%)	0.264



[子三]：建構安全智慧電表供應鏈韌體更新機制

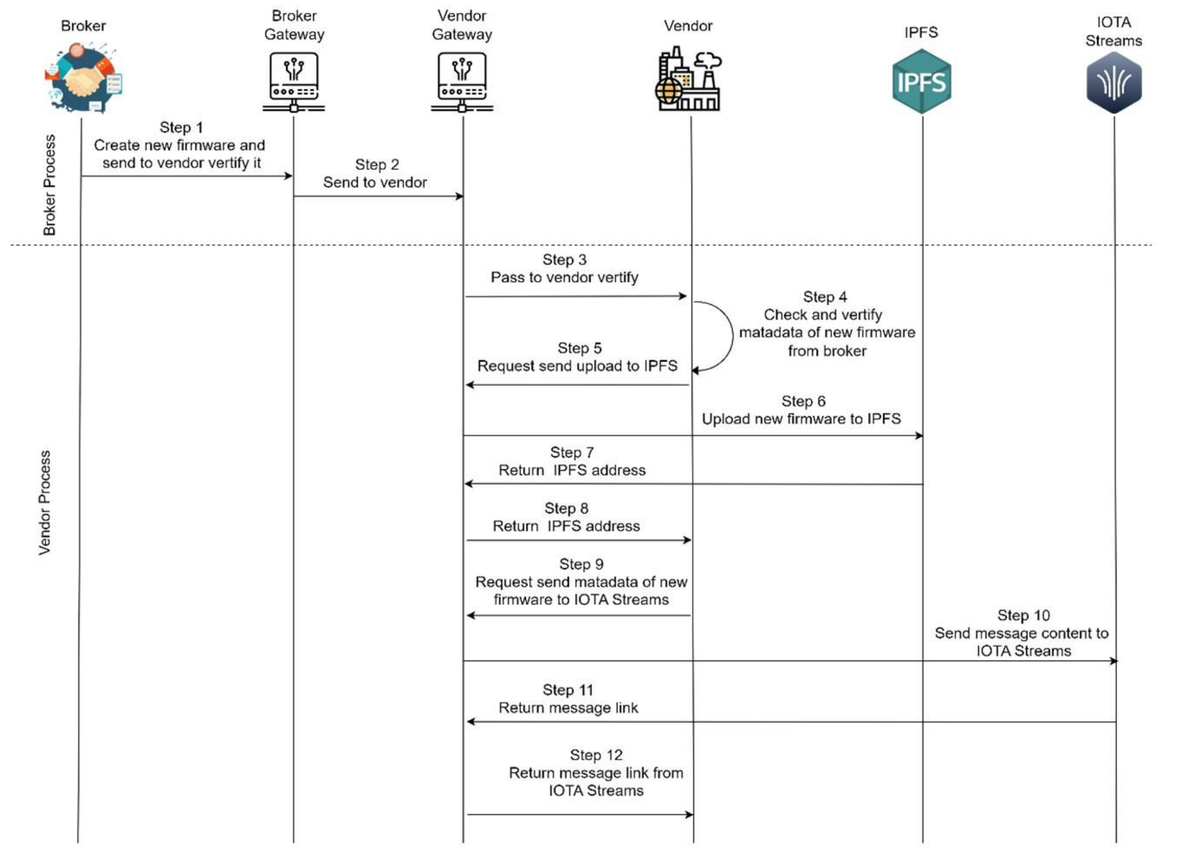
林詠章(中興資管)、王丕中(中興資工)、林家禎(勤益資工)

1. 技術摘要

利用IOTA分佈式帳本技術，來實現安全的工業物聯網設備軟體和韌體更新。透過IOTA Streams來發布更新訊息與IOTA分散式架構來儲存軟體和韌體更新文件，並設計了推式(PUSH)及拉式(PULL)的更新程序，以構建一個安全、可靠且高效的更新機制，確保所有更新文件的安全性和完整性，並大幅地降低系統更新過程受到攻擊的風險。

2.技術亮點/突破點：

Fig. 4. 新韌體更新檔案發布流程圖



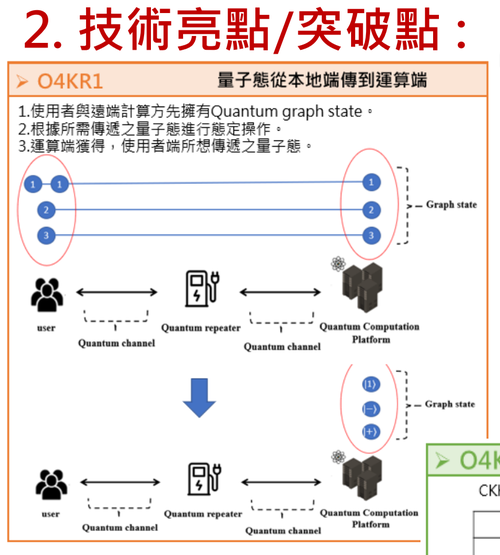
[子四]：同態加密技術於量子雲端運算之研究

林傑森(中興資工)、蔡家緯(中科大資工)

1. 技術摘要

同態加密演算法尋找適用於AI運算的潛在方案。由於各同態加密演算法適用的加密方法、運算效率、支援的數字範圍不盡相同，對於架構一個同態加密運用在AI雲端運算之系統如果要將同態加密做較為廣大的應用，現階段可以將計算切分為不同的部分，並提供不同的同態加密演算法，需要時在它們之間混合使用。為了深入探討在不同任務中同態加密技術之間的效能差異，本研究針將對 CKKS、BFV 及 TFHE 三種演算法進行效能比較。

2. 技術亮點/突破點：



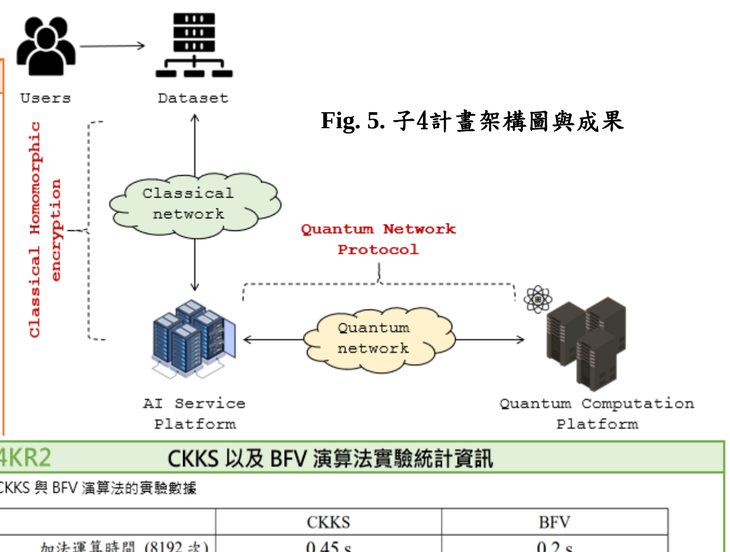
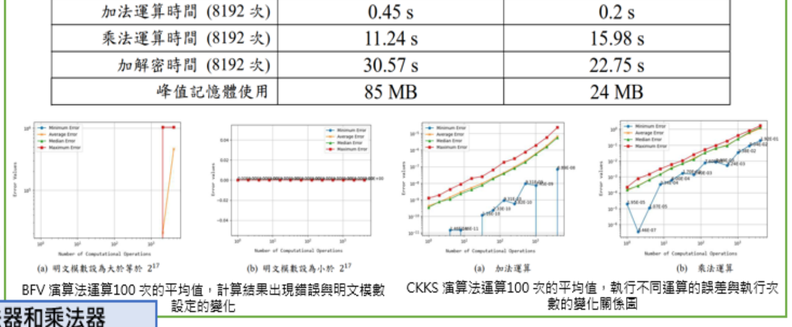


Fig. 5. 子4計畫架構圖與成果

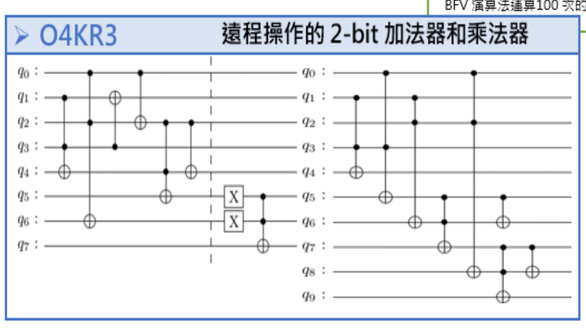


	CKKS	BFV
加法運算時間 (8192 次)	0.45 s	0.2 s
乘法運算時間 (8192 次)	11.24 s	15.98 s
加解密時間 (8192 次)	30.57 s	22.75 s
峰值記憶體使用	85 MB	24 MB

O4KR1:對 CKKS、BFV 同態加密演算法進行計算及加解密實驗分析其效能瓶頸。

O4KR2:設計以圖態為基礎的量子網路架構，並結合量子中繼器延長傳送距離。

O4KR3:在基於圖態的量子網路上，實現遠程的加法及乘法運算



[子五]：基於邊緣計算環境之異常檢測研究

歐陽彥杰(中興電機)、蔡國裕(逢甲資工)

1. 技術摘要

多變量時間序列異常檢測之模型研究，以物聯網的網路流量資料集做為檢測目標，提出有效的多變量時間序列無監督異常檢測模型。同時使用聯邦式學習進行模型的訓練與佈署，為確保訓練品質與防範相關攻擊，提出應用聲譽值抵抗中毒攻擊之聯邦式學習。結合兩者做為佈署邊緣異常檢測系統的完整訓練框架，增進實際應用的可能性。**基於:**

① **具抵抗中毒攻擊之聲譽值聯邦學習訓練框架**

② **雙向雙重閘門機制GRU-AE之物聯網多變量時間序列異常檢測模型**

2.技術亮點/突破點：

Fig. 6. 系統架構與流程圖

國立中興大學資通安全研究與教學中心TWISC@NCHU
402臺中市南區興大路145號應用科技大樓3樓319室
twiscnchu@nchu.edu.tw | 04-22840141#319

國立中興大學 NATIONAL CHUNG HSING UNIVERSITY